



12 Fragen zum Thema: Updates

Florian Brand – LinuxTag 2004

Agenda

- Grundlagen
- Risiken und Nebenwirkungen
- Sicherheit der Updates
- Verwaltung größerer Netzwerke

Frage 1:

Welche Updates müssen
eingespielt werden?

Nicht ob, sondern wann.

- Mythos: Unwichtiges System
- Sicherheitsupdates zeitnah einspielen
- Bugfixes nach Bedarf
- Nicht benutzte Software nicht installieren

Frage 2:

Welche Möglichkeiten habe ich Updates einzuspielen?

Drei Möglichkeiten

■ Neuübersetzung der Quellen

- sehr hoher administrativer Aufwand
- notwendig bei selbstangepasster Software

■ Binärpatches

- hoher Aufwand in der Verwaltung
- kurze Downloadzeiten

■ vollständige Pakete

- längere Downloadzeiten
- “Auslassen” von Updates möglich

Frage 3:

Bei welchen Paketen muss
ich besonders aufpassen?

Problematische Pakete

■ GLIBC:

- erfordert Neustart aller Daemons
- Reboot ratsam
- Vorsicht beim Updaten über das Netz

■ Kernel:

- Update löscht Module des alten Kernels
- Deshalb:
rpm -ivh kernel-`<version>`.`<arch>`.rpm

Frage 4:

Wird die Software nach dem
Updates noch einwandfrei
funktionieren?



Risiken bei Updates

- Veränderter Syntax der Konfiguration
- Inkompatibles API
- Datenverlust
- Ausfallzeiten bei Fehlschlag

Frage 5:

Wie testet man Updates?

Test der Updates

- Updates sollten zunächst auf einem identischen Testsystem aufgepielt werden.
- Anschliessender Test der Applikation(en)
- Aufwand rechnet sich nur bei unternehmenskritischen Systemen

Frage 6:

Was kann der Distributor für mich tun?

Backports

- Bugfixes werden in der Community durch neue Versionen realisiert.
- Neue Version bedeutet (oft) neue Features.
- Neue Features gefährden die Kompatibilität.
- Besser: Rückportierung des Bugfixes auf die ursprüngliche Version.
- Hoher Aufwand, sollte daher vom Distributor übernommen werden.

Frage 7:

Sind die herunter geladenen
Pakete fehlerfrei?

Frage 8:

Bin ich sicher, wenn der
Update Server gehackt
wird?



Paketsignaturen

- garantieren Echtheit der Pakete
- Schutz auch bei gehacktem Updateserver
- Test mit:
 # **rpm -K <Paket Datei>**
 foobar.rpm: (sha1) dsa sha1 md5 gpg OK
- Public Key des Distributors muss installiert sein: **rpm --import <PublicKey Datei>**

Frage 9:

Sind die Pakete auf meinem
System noch im
Originalzustand?

☐

Paket Verifizierung

- Vergleich des Dateisystems mit dem “Sollzustand” der RPM-Datenbank:

```
# rpm -V <Paket>
```

```
S.5....T c /etc/foobar.cfg
```

- Zeigt alle Veränderungen an.

- aber:

- Keine Kryptographische Sicherheit
- erkennt nur Dateien, die von RPM verwaltet werden

Frage 10:

Wie verringere ich den
Aufwand von Updates
in großen Netzwerken?



Strategien im Rechenzentrum

I

- Beseitigung von Sonderfällen
- Keine “händische Installation” auf Produktivmaschinen
- Eingekompilate vermeiden
- Eigene Software paketieren
- Automatisierung der Installation mit Kickstart

Frage 11:

Wie kann ich Updates
netzwerkweit automatisch
installieren?



Strategien im Rechenzentrum

II

- Bereithaltung der Software & Updates auf zentralem System
- Skriptgesteuertes Einspielen der Updates
- Zentrale “Inventarisierung” der Software

Frage 12:

Woher weiss ich auf
welchem Softwarestand
meine Systeme sind?



Beispiel: Red Hat Network

- Webbasierte Administration der Software Updates
- Datenbankgestützt
- Rechner können als Gruppe verwaltet werden
- Verwaltung von Konfigdateien möglich
- Kombination mit Kickstart
- Damit ist auch ein Recovery nach einem Ausfall möglich

Danke für Ihre Aufmerksamkeit!

- Slides:

<http://people.redhat.com/fbrand>

- Kontakt:

fbrand@redhat.com

- Frage 12b: Haben Sie Fragen?